UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/648,936	08/27/2003	Richard A. Steinmetz	D-1150 DIV	5940

28995 7590 02/13/2008

RALPH E. JOCKE
walker & jocke LPA
231 SOUTH BROADWAY
MEDINA, OH 44256

EXAMINER	
HAMILTON, LALITA M	

ART UNIT	PAPER NUMBER
3691	

MAIL DATE	DELIVERY MODE
02/13/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte RICHARD A. STEINMETZ, RICHARD P. BRUNT, and
KENNETH W. ZAHOREC

Appeal 2007-2870
Application 10/648,936
Technology Center 3600

Decided: February 13, 2008

Before TERRY J. OWENS, HUBERT C. LORIN, and
ANTON W. FETTING, *Administrative Patent Judges.*
FETTING, *Administrative Patent Judge*

DECISION ON APPEAL

STATEMENT OF CASE

Richard A. Steinmetz, Richard P. Brunt, and Kenneth W. Zahorec (Appellants) seek review under 35 U.S.C. § 134 of a Non-Final rejection of claims 13-24 and 28-34, the only claims pending in the application on appeal.

We have jurisdiction over the appeal pursuant to 35 U.S.C. § 6(b) (2002).

We AFFIRM-IN-PART.

The Appellants invented an automated banking machine configuration system that provides for the selective and secure activation and configuration of software components and operational parameters (Specification 1:5-8).

An understanding of the invention can be derived from a reading of exemplary claim 13, which is reproduced below [bracketed matter and some paragraphing added].

> 13. A method for configuring an automated banking machine comprising:
>
> a) receiving a certificate
>
> through operation of the banking machine;
>
> b) authenticating at least one digital signature
>
> associated with the certificate
>
> through operation of the banking machine;
>
> c) configuring the banking machine
>
> responsive to
>
> the certificate and
>
> authentication of the at least one digital signature in step (b).

This appeal arises from the Examiner's Non-Final Rejection, mailed April 24, 2006. The Appellants filed an Appeal Brief in support of the appeal on July 20, 2006. An Examiner's Answer to the Appeal Brief was

mailed on November 3, 2006. A Reply Brief was filed on December 27, 2006.

PRIOR ART

The Examiner relies upon the following prior art:

Dulude US 6,310,966 B1 Oct. 30, 2001

REJECTION

Claims 13-24 and 28-34 stand rejected under 35 U.S.C. § 102(e) as anticipated by Dulude.

ISSUES

The issue pertinent to this appeal is whether the Appellants have sustained their burden of showing that the Examiner erred in rejecting claims 13-24 and 28-34 under 35 U.S.C. § 102(e) as anticipated by Dulude.

The pertinent issue turns on whether Dulude describes configuring software as claimed.

FACTS PERTINENT TO THE ISSUES

The following enumerated Findings of Fact (FF) are believed to be supported by a preponderance of the evidence.

Claim Construction

01. The disclosure defines "configure" as encompassing the processes associated with either or both of configuring so as to enable carrying out desired functions and installing so as to enable

instructions to be available for use by a computer device (Specification 5:9-12).

02. The disclosure contains no lexicographic definition of a "licensing authority." The disclosure does state that a licensing authority *may* be a manufacturer of the automated banking machine or any other entity charged with managing the license provisions of automated banking machine software (Specification 6:13-16), but this is within the context of an embodiment, and is not definitive.

Dulude

03. Dulude is directed toward a biometric certification system binding the biometric identification of consumers with digital certificates. The biometric certification system authenticates electronic transactions involving a user, and includes a biometric input device which responds to a set of physical characteristics of the user, and generates corresponding biometric data related to the physical condition of the user. Biometric data is pre-stored as biometric certificates of registered users through a biometric input device. Subsequent transactions have transaction biometric data generated from the physical characteristics of a current user, which is then appended to the transaction data. The user is authenticated by comparison against the pre-stored biometric data of the physical characteristics of users in the biometric database (Dulude 3:31-50).

04. Dulude's biometric registration section processes user biometrics and associated inputs to generate biometric certificates which are unique to the user, and which are stored in a biometric database and/or a smart card memory. Once such biometric certificates are stored, a user may conduct biometrically-secured electronic transactions sent from the transaction transmission section to the transaction reception section of Dulude's FIG. 5, at which the electronic transaction is authenticated and processed (Dulude 4:17-25).

05. Dulude generates a certificate using a public key of the user at a certificate generator of a registration authority (Dulude 4:55-61).

06. Dulude's biometric certificates are stored in a memory, such as a biometric database or a memory of a smart card. Dulude's registration system may be located at a central registration station associated with a network, such that the corresponding biometric certificates of a user may be directly and securely stored in a central biometric database of a network or an individual memory of a smart card of the user. Accordingly, a central biometric database may serve a network of users conducting transactions, such as electronic commerce (E-commerce), over the Internet and other networks. Alternatively, a smart card of the user may pre-store the biometric certificates, such that kiosks and other devices such as terminals and automatic teller machines (ATMs) may obtain the secured biometric certificate of the user (Dulude 5:33-49).

07. Dulude's transaction data may include electronic funds transfers through an ATM (Dulude 5:56-59).

08. Dulude authenticates a user by sending a decrypted user public key of a certifying authority to decrypt the digital. The decryptor then extracts a hash value which was incorporated into the digital signature. The digital signature is authenticated by comparing hash values (Dulude (6:66 – 7:20).

PRINCIPLES OF LAW

Claim Construction

During examination of a patent application, pending claims are given their broadest reasonable construction consistent with the specification. *In re Prater*, 415 F.2d 1393, 1404-05 (CCPA 1969); *In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1364, (Fed. Cir. 2004).

Limitations appearing in the specification but not recited in the claim are not read into the claim. *E-Pass Techs., Inc. v. 3Com Corp.*, 343 F.3d 1364, 1369 (Fed. Cir. 2003) (claims must be interpreted "in view of the specification" without importing limitations from the specification into the claims unnecessarily)

Although a patent applicant is entitled to be his or her own lexicographer of patent claim terms, in *ex parte* prosecution it must be within limits. *In re Corr*, 347 F.2d 578, 580 (CCPA 1965). The applicant must do so by placing such definitions in the Specification with sufficient clarity to provide a person of ordinary skill in the art with clear and precise notice of the meaning that is to be construed. *See also In re Paulsen*, 30 F.3d 1475, 1480

(Fed. Cir. 1994) (although an inventor is free to define the specific terms used to describe the invention, this must be done with reasonable clarity, deliberateness, and precision; where an inventor chooses to give terms uncommon meanings, the inventor must set out any uncommon definition in some manner within the patent disclosure so as to give one of ordinary skill in the art notice of the change).

Anticipation

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987). "When a claim covers several structures or compositions, either generically or as alternatives, the claim is deemed anticipated if any of the structures or compositions within the scope of the claim is known in the prior art." *Brown v. 3M*, 265 F.3d 1349, 1351 (Fed. Cir. 2001). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236 (Fed. Cir. 1989). The elements must be arranged as required by the claim, but this is not an *ipsissimis verbis* test, i.e., identity of terminology is not required. *In re Bond*, 910 F.2d 831, 832 (Fed. Cir. 1990).

ANALYSIS

Claims 13-24 and 28-34 rejected under 35 U.S.C. § 102(e) as anticipated by Dulude.

The Appellants argue each of claims 13-23, 24 and 28 individually. We must initially construe the term "configure." The disclosure defines this

term using alternative definitions, *viz.* encompassing the processes associated with either or both of configuring so as to enable carrying out desired functions and installing so as to enable instructions to be available for use by a computer device (FF 01). We therefore construe "configure" according to the broadest of these alternatives, as enabling the carrying out of desired functions.

Claim 13

The Examiner found that Dulude anticipated claim 13 (Answer 3-4).

The Appellants contend that Dulude fails to show configuring responsive to a certificate and to signature authentication (Appeal Br. 14-15). The Examiner responded that Dulude describes the authentication (Dulude 4:10-25) by an ATM (Dulude 5:33-50), and configuring the ATM in response (Dulude 4:10-25; 5:33-50). The Appellant then argues that although Dulude describes signature authentication, it is not inherent that this is performed by the banking machine (Reply Br. 6:First and second full ¶'s).

We disagree with the Appellants. We find that Dulude describes authenticating a user by both a certificate and authentication of a digital signature (FF 08). Dulude authenticates a transaction, by means of authenticating a digital signature within a certificate, at its reception section (FF 04). For the embodiment of an ATM, this would be within the ATM itself, where such data is received. Dulude configures an ATM, in that Dulude enables the ATM to carry out a function, to process transactions such as electronic funds transfers, following authentication (FF 07).

Thus the Appellants have not sustained their burden of showing error in the rejection.

Claim 14

Claim 14 further requires that the certificate include the digital signature, which is authenticated responsive to a public key of a licensing authority.

The Examiner found that the data containing a certificate on Dulude's smart card embodiment is authenticated responsive to a public key of a registration authority (Answer 8).

The Appellants contend that Dulude decrypts with a user key, and Dulude does not describe this as a public key of a licensing authority, nor authenticating through operation of an ATM (Appeal Br. 16).

We disagree. Dulude generates a certificate on Dulude's smart card embodiment responsive to a public key of a registration authority (FF 05). Dulude's data containing a certificate on Dulude's smart card embodiment is authenticated responsive to a public key of a certifying authority (FF08). Although claim 14 requires that the public key be of a licensing authority, the Specification does not define a licensing authority (FF 02). We therefore construe a licensing authority according to its broadest reasonable interpretation. We find that the processes of registration and certification each imply licensing of that which is registered or certified, and therefore that Dulude's registration and certifying authorities are examples of licensing authorities.

Thus the Appellants have not sustained their burden of showing error in the rejection.

Claim 15

Claim 15 further requires that the certificate correspond to at least one software component authorized to be installed on the banking machine, and installing the software component on the banking machine.

The Examiner found that the certificates on smart cards are software and the act of inserting the card in a machine installs the card's memory containing the data on the card (Answer 8). The Appellants contend that Dulude fails to show installing a software component in response to authorization (Appeal Br. 16-17).

We agree. Even if we were to construe inserting a card containing memory as an installation, as the Examiner did, such an insertion would not be in response to the authentication, but only to the insertion of the card. Further, although the certificate on a smart card might be characterized as software, it is input data, not a component of the machine's software.

Thus the Appellants have sustained their burden of showing error in the rejection.

Claim 16

Claim 16 further requires that the certificate include sets of configuration rules, each set corresponding to an automated banking machine which is enabled to be configured responsive to at least one set.

The Examiner found that the certificate on a smart card has rules for its use in kiosks or ATM's (Answer 9). The Appellants contend that Dulude fails to describe plural rules corresponding to at least one of plural banking

machines, the machines configured to be responsive to at least one set of rules (Appeal Br. 18).

We agree. Dulude does not describe any rules being contained within its certificates. The rules which the Examiner describes are those within the ATM, not within Delude's certificate.

Thus the Appellants have sustained their burden of showing error in the rejection.

Claim 17

Claim 17 further requires determining through operation of the banking machine responsive to an expiration parameter that configuration of the software on the machine is not authorized and so preventing configuration of software on the banking machine.

The Examiner found that Dulude describes certificates having validity periods for authorization (Answer 9). The Appellants contend that irrespective of such validity periods, Dulude fails to describe their use in authorizing the configuration of software on the machine (Appeal Br. 9).

We agree. Unlike claim 13 which configures a machine, claim 17 requires determining whether configuration *of software* on a machine is authorized. Thus, whereas configuring a machine to operate met the breadth of claim 13, because changing a machine's state meets the broad construction of "configure", this would be insufficient to show determining whether configuration of software is authorized. Changing the configuration of software requires actually changing the interrelationships of software

components. The Examiner has not shown where Dulude describes this, and we have similarly been unable to find any such description within Dulude.

Thus the Appellants have sustained their burden of showing error in the rejection.

Claims 18-21

Claim 18 further requires that the certificate includes an identification value unique to the banking machine.

Claim 19 further requires determining through operation of the banking machine that the identification value corresponds to a hardware embedded identification value in the banking machine.

Claim 20 further requires that the certificate include a terminal identification value and associating the machine with the terminal identification value.

Claim 21 further requires determining that the terminal identification value has changed and preventing the machine from performing at least one transaction function.

The Examiner found that Dulude describes identifying data (Answer 10). The Appellants contend that the information pointed to by the Examiner is not unique to the machine or terminal (Appeal Br. 19-21).

We agree. The identification data pointed to by the Examiner (Dulude 1:65-2:15) refers to user, card, or certificate identification, not to a banking machine or terminal.

Thus the Appellants have sustained their burden of showing error in the rejections of claims 18-21.

Claims 22 and 23

Claims 22 and 23 further require receiving the certificate from a licensing authority or from a server in operative connection with the banking machine.

The Examiner found that Dulude received the certificate from a smart card, provided by a licensing authority and using a server (Answer 11). The Appellants contend that does not describe these features.

We disagree. As we found with claim 14, *supra*, the certificate on Dulude's smart card is from a licensing authority. We further find that Dulude describes a network alternate embodiment (Dulude Fig. 5) which would provide the certificate from a server.

Thus the Appellants have not sustained their burden of showing error in the rejection.

Claim 24

Claim 24 is the same subject matter of claim 13 drafted in the form of computer media bearing instructions for performing the method of claim 13. The Appellants contend that claim 24 is patentable for the same reasons as claim 13, *supra*. We found the Appellant did not meet the burden of showing error in the rejection of claim 13, *supra*, and thus the Appellants have not sustained their burden of showing error in the rejection.

Claims 28-34

Claim 28 is independent and requires verifying through operation of at least one processor that the at least one serial number included in the at least one certificate corresponds to at least one serial number associated with at least one hardware device of the ATM.

The Examiner found that Dulude described using the serial numbers in smart cards to determine which devices might access the user certificates (Answer 13-14). The Appellants contend that Dulude does not describe at least one serial number included in the at least one certificate corresponds to at least one serial number associated with at least one hardware device of the ATM (Appeal Br. 25).

We agree. The portion of Dulude cited by the Examiner (Dulude 2:1-10; 5:40-50) merely describes allowing operation of an ATM following validation of the certificate on a smart card. We find nothing in Dulude that describes relying on a serial number associated with at least one hardware device of an ATM.

Thus the Appellants have sustained their burden of showing error in the rejection of claim 28, and accordingly, in the claims 29-34 that depend from claim 28 as well.

CONCLUSIONS OF LAW

The Appellants have sustained their burden of showing that the Examiner erred in rejecting claims 15-21 and 28-34, but have not sustained their burden of showing that the Examiner erred in rejecting claims 13, 14, 22, 23 and 24 under 35 U.S.C. § 102(e) as unpatentable over the prior art.

DECISION

To summarize, our decision is as follows:

- The rejection of claims 13, 14, 22, 23 and 24 under 35 U.S.C. § 102(e) as anticipated by Dulude is sustained.
- The rejection of claims 15-21 and 28-34 under 35 U.S.C. § 102(e) as anticipated by Dulude is not sustained.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED-IN-PART

vsh

RALPH E. JOCKE
WALKER & JOCKE LPA
231 SOUTH BROADWAY
MEDINA OH 44256